

IFW/AF
2161

PTO/SB/21 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission

Application Number	10/016,700
Filing Date	11/02/2001
First Named Inventor	Challener et al.
Art Unit	2161
Examiner Name	Cindy Nguyen
Attorney Docket Number	RPS920000400US2

ENCLOSURES (Check all that apply)

<input checked="" type="checkbox"/> Fee Transmittal Form	<input type="checkbox"/> Drawing(s)	<input type="checkbox"/> After Allowance Communication to TC
<input checked="" type="checkbox"/> Fee Attached	<input type="checkbox"/> Licensing-related Papers	<input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences
<input type="checkbox"/> Amendment/Reply	<input type="checkbox"/> Petition	<input checked="" type="checkbox"/> Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
<input type="checkbox"/> After Final	<input type="checkbox"/> Petition to Convert to a Provisional Application	<input type="checkbox"/> Proprietary Information
<input type="checkbox"/> Affidavits/declaration(s)	<input type="checkbox"/> Power of Attorney, Revocation	<input type="checkbox"/> Status Letter
<input type="checkbox"/> Extension of Time Request	<input type="checkbox"/> Change of Correspondence Address	<input checked="" type="checkbox"/> Other Enclosure(s) (please identify below):
<input type="checkbox"/> Express Abandonment Request	<input type="checkbox"/> Terminal Disclaimer	Return Postcard
<input type="checkbox"/> Information Disclosure Statement	<input type="checkbox"/> Request for Refund	
<input type="checkbox"/> Certified Copy of Priority Document(s)	<input type="checkbox"/> CD, Number of CD(s) _____	
<input type="checkbox"/> Reply to Missing Parts/Incomplete Application	<input type="checkbox"/> Landscape Table on CD	
<input type="checkbox"/> Reply to Missing Parts under 37 CFR 1.52 or 1.53		

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Winstead Sechrest & Minick P.C.		
Signature			
Printed name	Kelly K. Kordzik		
Date	4/19/2005	Reg. No.	36,571

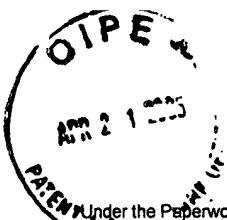
CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name	Toni Stanley	Date	4/19/2005

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



PTO/SB/17 (11-04)

Approved for use through 07/31/2006. OMB 0651-0032

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Effective on 10/01/2004. Patent fees are subject to annual revision.

FEE TRANSMITTAL

For FY 2005

☐ Applicant claims small entity status. See 37 CFR 1.27**TOTAL AMOUNT OF PAYMENT (\$)** 500.00**Complete if Known**

Application Number	10/016,700
Filing Date	11/02/2001
First Named Inventor	Challener et al.
Examiner Name	Cindy Nguyen
Art Unit	2161
Attorney Docket No.	RPS920000400US2

METHOD OF PAYMENT (check all that apply)☐ Check ☐ Credit Card ☐ Money Order☒ Deposit Account ☐ None

Deposit Account Number: 50-0563
Deposit Account Name: IBM Corporation

The Director is hereby authorized to: (check all that apply)

- ☒ Charge fee(s) indicated below
☐ Charge fee(s) indicated below, except for the filing fee
☒ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17
☒ Credit any overpayments

to the above-identified deposit account.

☐ Other (please identify):

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION**1. BASIC FILING FEE**

Fee Description	Fee (\$)	Small Entity Fee (\$)	Fee Paid (\$)
Utility Filing Fee	790	395	
Design Filing Fee	350	175	
Plant Filing Fee	550	275	
Reissue Filing Fee	790	395	
Provisional Filing Fee	160	80	

Subtotal (1) \$**FEE CALCULATION** (continued)**2. EXTRA CLAIM FEES**

Fee Description	Fee (\$)	Small Entity Fee (\$)
Each claim over 20	50	25
Each independent claim over 3	200	100
Multiple dependent claims	360	180
For Reissues, each claim over 20 and more than in the original patent	50	25
For Reissues, each independent claim more than in the original patent	200	100

Total Claims **Extra Claims** **Fee (\$)** **Fee Paid (\$)**
- 20 or HP = _____ x _____ = _____
HP = highest number of total claims paid for, if greater than 20

Indep. Claims **Extra Claims** **Fee (\$)** **Fee Paid (\$)**
- 3 or HP = _____ x _____ = _____
HP = highest number of independent claims paid for, if greater than 3

Multiple Dependent Claims **Fee (\$)** **Fee Paid (\$)**

Subtotal (2) \$**3. OTHER FEES**

Fee Description	Fee (\$)	Small Entity Fee (\$)	Fee Paid (\$)
1-month extension of time	120	60	
2-month extension of time	450	225	
3-month extension of time	1,020	510	
4-month extension of time	1,590	795	
5-month extension of time	2,160	1,080	
Information disclosure stmt. fee	180	180	
37 CFR 1.17(q) processing fee	50	50	
Non-English specification	130	130	
Notice of Appeal	500	250	
Filing a brief in support of appeal	500	250	500.00
Request for oral hearing	1,000	500	
Other:			

Subtotal (3) \$ 500.00**SUBMITTED BY**

Signature

Registration No.
(Attorney/Agent)

36.571

Telephone 512-370-2851

Name (Print/Type)

Kelly K. Kordzik

Date 4/19/2005

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



RPS9-2000-0400US2

PATENT

- 1 -

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of: : Before the Examiner:
Challener et al. : Cindy Nguyen
Serial No.: 10/016,700 : Group Art Unit: 2161
Filed: November 2, 2001 :
Title: TRUSTED COMPUTING PLAT- : IBM Corporation
FORM WITH DUAL KEY TREES TO : P.O. Box 12195
SUPPORT MULTIPLE PUBLIC/PRIVATE : Dept. T81/B503
KEY SYSTEMS : Research Triangle Park, NC 27709

APPEAL BRIEF

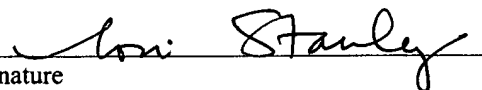
Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

I. **REAL PARTY IN INTEREST**

The real party in interest is International Business Machines Corporation, which is the assignee of the entire right, title and interest in the above-identified patent application.

CERTIFICATION UNDER 37 C.F.R. §1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450, on April 19, 2005.


Signature

Toni Stanley
(Printed name of person certifying)

04/22/2005 EFLDRES 00000050 500563 10016700
01 FC:1402 500.00 DA

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellants, Appellants' legal representative or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1-8, 18-24 and 27 are pending in the application. Claims 9-17 have been allowed. Claims 1-6, 8, 18-25 and 27 stand rejected. Claims 7 and 26 are objected to.

IV. STATUS OF AMENDMENTS

Applicants have filed an Amendment After Final amending claims 7 and 26 to be in independent form.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Referring to FIGURE 5, there is illustrated an embodiment of the present invention for the creation and use of keys within a TPM, such as TPM 951 described below with respect to FIGURE 9. There is a TPM storage root key 501 and a platform migratable key 502. Additionally, there are user migratable keys 503 and 504 and signing keys 507 thereunder. All such keys are migratable. The present invention, however, makes use of the ability of a TPM to have non-migratable keys as well as migratable keys. Migratable keys can be transferred to other TPMs, and non-migratable keys cannot be transferred. Thus, such non-migratable keys are locked to the hardware, i.e., the TPM 951. With such non-migratable keys, the TPM 951 can only decrypt such keys. [Page 8, lines 10-19]

Such migratable and non-migratable keys are desired within the TPM, but the use of deeply embedded migratable keys is not desired because it takes too long for such embedded key structures to load. But yet, it is desirable to have such keys migratable for maintenance purposes, such as to move a single user from one platform to another or to move an entire platform from one system to another. It is not desirable in such instances to go through the system and find every single key, to determine what kind of key it is and then migrate such keys individually. [Page 8, line 20 – page 9, line 4]

As noted above, deeply embedded trees of keys take a relatively long time to load. For example, if it is desired to have a signing key, then that signing key will be encrypted with a public key of a user key, which may be encrypted with the key of a department, which may be encrypted with key of the platform which is encrypted with the storage root key. All such keys within the tree need to be loaded. However, since it is not desirable that every member of a department have access to the keys of every user in that department, individual user authentication data may be associated with each user key, so that only the appropriate user is allowed to load keys associated with that user. This is especially the case as a given "leaf" key may be set to not use user authentication data in order to be used, so loading the key in this case is equivalent to being able to use the key. Ease of use and security constraints dictate that there not be two sets of user authentication data for loading a key. [Page 9, lines 5-16]

Referring to FIGURE 6, in the present invention, in step 601, a new migratable signing key is created. Then, in step 602, the new migratable signing key is stored in the user migratable storage key 503 or 504. In step 603, the new migratable signing key is also stored in the user non-migratable storage key 505 or 506. By design, the same user authentication data is used to perform this action for both storage keys, so the user only needs to provide it once. Since the user non-

migratable storage key 505 or 506 is the faster type of public/private key, it will load faster when the migratable signing key is needed. [Page 10, lines 3-10]

In a similar way, when a new migratable storage key is requested to be created and stored under a specified migratable storage key M, the request will be translated into two requests. The first will behave exactly as specified by the TCPA specification. The second request will request a non-migratable storage key (of faster type) to be created and stored under the non-migratable storage key corresponding to M in the fast tree. Both requests will contain the same user authorization data, and then the database on the system which associates migratable storage keys and non-migratable storage keys will be updated to reflect the new correspondence between the two newly created keys. [Page 10, lines 11-19]

Referring to FIGURE 7, in step 701, a request for a signature by a key is made. In step 702, the database is searched for the location of the key blob to load. In step 703, a copy of the key stored in the non-migratable storage key blob is loaded, and in step 704, the key is used to execute the signature. [Page 11, lines 7-10]

In the present invention, in FIGURE 8, in step 801, a migration of a key is requested. In step 802, the database is searched for the location of the key blob to load. In step 803, a copy of the key stored in the non-migratable storage key blob is loaded, and this key is used to sign in step 804. The present invention allows users to store and load keys much more quickly with faster public/private keys than 2048 bit RSA keys. However, the present invention preserves both the ability to migrate keys and also the structure of user authentication data needed to load or use a key. [Page 12, lines 11-19]

VI. GROUND OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-6, 18-25 and 27 stand rejected under 35 U.S.C. § 102(e) as being anticipated by David Grawrock "TCPA TPMPP" version 0.45, September 14, 2000 (hereinafter "Grawrock").

VII. ARGUMENT

Claims 1-6, 8, 18-25 and 27 are not properly rejected under 35 U.S.C. § 102(e) as being anticipated by David Grawrock "TCPA TPMPP" version 0.45, September 14, 2000 (hereinafter referred to as "Grawrock"). As the Examiner is well aware, for a claim to be anticipated under § 102, each and every element of the claim must be found within the cited prior art reference. As Applicant will hereinafter assert, the Examiner has not sufficiently shown where in Grawrock the various limitations of the claims are found. Though an examiner may give claim language a broad interpretation, such an interpretation must be reasonable, and also consistent with the interpretation that those skilled in the art would reach, taking into account whatever enlightenment by way of definitions or otherwise that may be afforded by the written description contained in Applicant's Specification. MPEP § 2111.

A migratable key can be transferred to other trusted platform modules chips, while non-migratable keys cannot be transferred. Specification, page 8, lines 16-17. Thus, such non-migratable keys are locked to the hardware, which is the only hardware that can decrypt such keys. Specification, page 8, lines 17-19.

A. Claims 1 and 18

With respect to claims 1 and 18, the Examiner has asserted that page 18 of Grawrock teaches the claim limitations in claims 1 and 18. Applicant respectfully traverses. The Grawrock reference merely refers to the target of evaluation that must provide the mechanisms to identify the tree a storage entity is in (migratable or non-migratable). However, this language does not teach creating a migratable storage tree

with a storage root key. Nothing within Grawrock teaches creating a non-migratable storage tree with the storage root key, wherein the migratable storage tree and the non-migratable storage tree are identically structured. All that the Examiner has found in Grawrock are the words TCPA, key, migratable and non-migratable. But the claims recite more than just these words, which the rejections fail to properly address. Moreover, the language cited by the Examiner on page 67 of Grawrock also merely mentions the terms migratable and non-migratable, but does not in any way teach or suggest the specific claim recitations.

B. Claim 18

Furthermore, with respect to claim 18, the additional limitations within that claim that the migratable storage tree and the non-migratable storage tree are identically structured with corresponding keys and authentication data is not in any way disclosed in page 18 of Grawrock.

C. Claims 2 and 19

Claims 2 and 19 recite that the migratable storage tree and the non-migratable storage tree are created by a trusted computing module in accordance with the Trusted Computing Platform Alliance. The Examiner has attempted to reject these claims by citing all of page 6 of Grawrock. There is absolutely no disclosure of a trusted computing module on page 18 of Grawrock.

D. Claims 3 and 20

With respect to claims 3 and 20, these claims recite that the migratable storage tree comprises migratable keys and a user key, wherein the non-migratable storage tree comprises non-migratable keys and a user key. The Examiner has attempted to reject these claims by citing pages 19-20 of Grawrock. The Examiner has failed to specifically point out on these pages where these limitations are found, and instead

has made a blanket assertion using applicants claim language, but not citing to any specific Grawrock language.

In the Examiner's final rejection, the Examiner has responded as follows:

In response, Grawrock clearly discloses: migratable storage tree comprises migratable keys and user key, wherein the non-migratable storage tree comprises non-migratable keys and a user key as user access control policy is the user key, encrypted data between data and keys, Eencrypted [sic] keys is the non-migratable keys that no way for data to enter the key handling module, also all the keys defined in page 19 are provided by TCPA for security transfer protect cryptographic data assets when they are being transmitted to and from the TOE see page whole page 19.

In response, Applicants don't even understand what the Examiner is trying to say; the Examiner's response is incoherent.

E. Claims 4 and 22

With respect to claims 4 and 22, these claims recite that the non-migratable storage tree will include non-migratable storage keys corresponding to each migratable storage key in the migratable storage tree. In rejecting these claims, the Examiner has recited page 26 of Grawrock. There's absolutely no teaching or inference of non-migratable storage trees having non-migratable storage keys corresponding to migratable storage keys in a migratable storage tree. The Examiner needs to point to specific language on page 26 of Grawrock, and not just cite the whole page. Furthermore, the Examiner has cited pages 67-78 of Grawrock in the Examiner's final rejection. Again, the Examiner cannot cite to several whole pages without specifically pointing out how the claim language specifically teaches what is recited in the claims.

F. Claims 5 and 24

With respect to claims 5 and 24, these claims recite that use authorization in the non-migratable storage tree will be identical to use authorization in the migratable storage tree. The Examiner has attempted to reject these claims by referring to page 16 of the Grawrock reference. Again, the Examiner's rejection amounts to merely citing a whole page of a reference and then not comparing the claim language to any specific language on this page, which is wholly inadequate to support a *prima facie* case of anticipation.

In the Examiner's final rejection, the Examiner has responded as follows:

In response, Grawrock clearly discloses: wherein use authorization in the non-migratable storage tree will be identical to use authorization in the migratable storage tree as for security transfer, TOE provide a protected storage mechanism for migration and non-migration the tree a storage entity, migration and non-migratable labels set never changes therefore they are identical to use authorization, see page 67-68.

First, Applicants do not understand what the Examiner is trying to say with this disjointed sentence. Secondly, the Examiner has not specifically pointed to any language in Grawrock that addresses the specific claim language.

G. Claim 6

Claim 6 recites the further steps of requesting a migratable storage tree and requesting a non-migratable storage key. Page 18 of Grawrock does not even remotely disclose these limitations.

H. Claim 8

Claim 8 recites the step of when a key loading request is made for a migratable storage key, loading a key from the non-migratable storage tree instead of

loading a corresponding key from the migratable storage tree. The Examiner has responded as follows:

In addition, Grawrock discloses: further comprising the steps of: when a key loading request is made for a migratable storage key, loading a key from the non-migratable storage key instead of loading a corresponding key from the migratable storage tree as the commands O.Input_inspection and O.Integ_data mark is require for downloads and transfer with another trusted product by using a protocol for data transfer that will permit error detection and correction see page 21.

First of all, Applicants do not understand what the Examiner is attempting to say with this disjointed sentence. Furthermore, the Applicant does not in any way describe how the O.Input_inspection and O.Integ_data commands address these claim limitations.

I. Claim 21

With respect to claim 21, pages 19-20 of Grawrock do not in any way disclose these limitations, and the Examiner has failed to show how they do.

J. Claim 23

With respect to claim 23, the Examiner has not compared the claims to any specific language in page 28 of Grawrock.

K. Claims 25 and 27

Grawrock does not teach the limitations of claim 25 that the use authorization in the non-migratable storage tree can be deduced from user authorization in the migratable storage tree with additional data. The Examiner cannot support a *prima facie* case of anticipation with the blanket rejection provided. The same is true for claim 27.

RPS9-2000-0400US2

PATENT

Respectfully submitted,

WINSTEAD SECHREST & MINICK P.C.

Attorneys for Appellants

By: 

Kelly K. Kordzik
Reg. No. 36,571

P.O. Box 50784
Dallas, Texas 75201
(512) 370-2832

APPENDIX

- 1 1. In a data processing system, a method comprising the steps of:
2 creating a migratable storage tree with a storage root key; and
3 creating a non-migratable storage tree with the storage root key, wherein the
4 migratable storage tree and the non-migratable storage tree are identically structured.
- 1 2. The method as recited in claim 1, wherein the migratable storage tree and the
2 non-migratable storage tree are created by a trusted computing module in accordance
3 with Trusted Computing Platform Alliance.
- 1 3. The method as recited in claim 1, wherein the migratable storage tree
2 comprises migratable keys and a user key, wherein the non-migratable storage tree
3 comprises non-migratable keys and a user key.
- 1 4. The method as recited in claim 1, wherein the non-migratable storage tree will
2 include non-migratable storage keys corresponding to each migratable storage key in
3 the migratable storage tree.
- 1 5. The method as recited in claim 1, wherein use authorization in the
2 non-migratable storage tree will be identical to use authorization in the migratable
3 storage tree.
- 1 6. The method as recited in claim 1, further comprising the steps of:
2 requesting a migratable storage key; and
3 requesting a non-migratable storage key.
- 1 7. The method as recited in claim 6, wherein the step of requesting a migratable
2 storage key will identify a parent key in the migratable storage tree, and wherein the

1 step of requesting a non-migratable storage key will identify a parent key in the
2 non-migratable storage tree that corresponds to the parent key in the migratable
3 storage tree.

1 8. The method as recited in claim 1, further comprising the step of:
2 when a key loading request is made for a migratable storage key, loading a
3 key from the non-migratable storage tree instead of loading a corresponding key from
4 the migratable storage tree.

1 9. In a data processing system, a method comprising the steps of:
2 splitting a request to create a new migratable storage key with given
3 authentication data and a first parent key into first and second commands;
4 wherein the first command creates a migratable storage key with the given
5 authentication data and the first parent key; and
6 wherein the second command requests creating a non-migratable storage key
7 with the given authentication data and a second parent key which is determined from
8 looking up a key that corresponds to the first parent key in a database.

1 10. The method recited in claim 9, wherein the migratable storage key and the
2 non-migratable storage key are associated in a database.

1 11. The method recited in claim 9, wherein the non-migratable key is a multi-
2 prime key.

1 12. The method recited in claim 9, where the non-migratable key is an elliptic
2 curve key.

1 13. The method as recited in claim 9, further comprising the steps of:
2 creating a new migratable signing key with the given authentication data and a
3 third parent key;
4 storing the new migratable signing key with the given authentication data and
5 the third parent key;
6 storing the new migratable signing key with the given authentication data and
7 a fourth parent key where the fourth parent key is a non-migratable key associated
8 with the third parent key in a database.

1 14. The method as recited in claim 13, further comprising the steps of:
2 requesting a signature by the new migratable signing key;
3 searching the database for the location of a key blob containing the new
4 migratable signing key;
5 loading a copy of the new migratable signing key stored in the key blob
6 created with the non-migratable parent key; and
7 signing with the new migratable signing key.

1 15. The method as recited in claim 9, further comprising the steps of:
2 creating a new data stored by means of the first parent key;
3 storing the new data with the first parent key;
4 storing the new data with the second parent key where the second parent key
5 is a non-migratable key associated with the third parent key in a database.

1 16. The method as recited in claim 15, further comprising the steps of:
2 requesting data stored by the new migratable storage key;
3 searching the database for the location of a key blob associated with the new
4 migratable storage key;
5 loading a copy of the key blob created with the non-migratable storage key;
6 and decrypting the data.

- 1 17. The method as recited in claim 14, further comprising the steps of:
2 requesting migration of new migratable signing keys;
3 searching the database for the location of a key blob associated with a non-
4 migratable parent of the key to be migrated;
5 processing the migration.
- 1 18. In a data processing system, a method comprising the steps of:
2 creating a migratable storage tree with a storage root key; and
3 creating a non-migratable storage tree with the storage rootkey where the
4 migratable storage tree and the non-migratable storage tree are identically structured
5 with corresponding keys and authentication data.
- 1 19. The method as recited in claim 18, wherein the migratable storage tree and the
2 non-migratable storage tree are created by a trusted computing module in accordance
3 with Trusted Computing Platform Alliance.
- 1 20. The method as recited in claim 19, wherein the migratable storage tree
2 comprises migratable keys and a user key, wherein the non-migratable storage tree
3 comprises non-migratable keys and a user key.
- 1 21. The method recited in claim 18, wherein the migratable storage tree comprises
2 migratable keys and encrypted user data wherein the non-migratable storage tree
3 comprises non-migratable keys and encrypted user data .
- 1 22. The method as recited in claim 18, wherein the non-migratable storage tree
2 will include non-migratable storage keys corresponding to each migratable storage
3 key in the migratable storage tree.

1 23. The method as recited in claim 18, wherein the non-migratable storage tree
2 will include non-migratable storage keys corresponding to a subset of the migratable
3 storage keys in the migratable storage tree.

1 24. The method as recited in claim 18, wherein use authorization in the non-
2 migratable storage tree will be identical to use authorization in the migratable storage
3 tree.

1 25. The method as recited in claim 18, wherein use authorization in the non-
2 migratable storage tree can be deduced from user authorization in the migratable
3 storage tree with additional data.

1 26. The method as recited in claim 25, wherein the use authorization in the non-
2 migratable storage tree is obtained by hashing the concatenation of the user
3 authorization in the migratable storage tree with a fixed string.

1 27. The method as recited in claim 1, wherein a migratable key can be transferred
2 to other trusted platform module chips, and wherein a non-migratable key cannot be
3 transferred to other trusted platform module chips.